

# Quantified Differential Temporal Dynamic Logic for Verifying Properties of Distributed Hybrid Systems<sup>\*</sup>

Ping Hou

Computer Science Department, Carnegie Mellon University

**Abstract.** We combine quantified differential dynamic logic (Qd $\mathcal{L}$ ) for reasoning about the possible behavior of distributed hybrid systems with temporal logic for reasoning about the temporal behavior during their operation. Our logic supports verification of temporal and non-temporal properties of distributed hybrid systems and provides a uniform treatment of discrete transitions, continuous evolution, and dynamic dimensionality-changes. For our combined logic, we generalize the semantics of dynamic modalities to refer to hybrid traces instead of final states. Further, we prove that this gives a conservative extension of Qd $\mathcal{L}$  for distributed hybrid systems. On this basis, we provide a modular verification calculus that reduces correctness of temporal behavior of distributed hybrid systems to non-temporal reasoning, and prove that we obtain a complete axiomatization relative to the non-temporal base logic Qd $\mathcal{L}$ . Using this calculus, we analyze temporal safety properties in a distributed air traffic control system where aircraft can appear dynamically.

## 1 Introduction

Ensuring correct functioning of cyber-physical systems is among the most challenging and most important problems in computer science, mathematics, and engineering. Hybrid systems are common mathematical models for cyber-physical systems with interacting discrete and continuous behavior [6,13]. Their behavior combines continuous evolution (called *flow*) characterized by differential equations and discrete jumps. However, not all relevant cyber-physical systems can be modeled as hybrid systems. Hybrid systems cannot represent physical control systems that are distributed or form a multi-agent system, e.g., distributed car control systems [15] and distributed air traffic control systems [8]. Such systems form *distributed hybrid systems* [7,16,21,22] with discrete, continuous, structural, and dimension-changing dynamics. Distributed hybrid systems combine the challenges of hybrid systems and distributed systems. Correctness of safety-critical real-time and distributed hybrid systems depends on a safe operation throughout *all* states of all possible trajectories, and the behavior at intermediate states is highly relevant [1,4,6,11,13].

---

<sup>\*</sup> This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246, Grant Nos. CNS-0926181, CNS-0931985, and CNS-1035800.

*Temporal logics* (TL) use temporal operators to talk about intermediate states [1,9,10,23]. They have been used successfully in model checking [1,3,13,14,18] of finite-state system abstractions. State spaces of distributed hybrid systems, however, often do not admit equivalent finite-state abstractions [13,18]. Instead of model checking, TL can also be used deductively to prove validity of formulas in calculi [5,6]. Valid TL formulas, however, only express very generic facts that are true for all systems, regardless of their actual behavior. Hence, the behavior of a specific system first needs to be axiomatized declaratively to obtain meaningful results. Then, however, the correspondence between actual system operations and a declarative temporal representation may be questioned.

Very recently, a dynamic logic, called *quantified differential dynamic logic* (QdL) has been introduced as a successful tool for deductively verifying distributed hybrid systems [21,22]. QdL can analyze the behavior of actual distributed hybrid system models, which are specified operationally. Yet, operational distributed hybrid system models are *internalized* within QdL formulas, and QdL is closed under logical operators. However, QdL only considers the behavior of distributed hybrid systems at final states, which is insufficient for verifying safety properties that have to hold all the time.

We close this gap of expressivity by combining QdL with temporal logic [9,10,23]. In this paper, we introduce a logic, called *quantified differential temporal dynamic logic* (QdTL), which provides modalities for quantifying over traces of distributed hybrid systems based on QdL. We equip QdTL with temporal operators to state what is true all along a trace or at some point during a trace. In this paper, we modify the semantics of the dynamic modality  $[\alpha]$  to refer to all *traces* of  $\alpha$  instead of all final states reachable with  $\alpha$  (similarly for  $\langle\alpha\rangle$ ). For instance, the formula  $[\alpha]\Box\phi$  expresses that  $\phi$  is true at each state during all traces of the distributed hybrid system  $\alpha$ . With this, QdTL can also be used to verify temporal statements about the behavior of  $\alpha$  at intermediate states during system runs. As in our non-temporal dynamic logic QdL [21,22], we use *quantified hybrid programs* as an operational model for distributed hybrid systems, since they admit a uniform compositional treatment of interacting discrete transitions, continuous evolutions, and structural/dimension changes in logic.

As a semantical foundation for combined temporal dynamic formulas, we introduce a hybrid trace semantics for QdTL. We prove that QdTL is a conservative extension of QdL: for non-temporal specifications, trace semantics is equivalent to the non-temporal transition semantics of QdL [21,22].

As a means for verification, we introduce a sequent calculus for QdTL that successively reduces temporal statements about traces of quantified hybrid programs to non-temporal QdL formulas. In this way, we make the intuition formally precise that temporal safety properties can be checked by augmenting proofs with appropriate assertions about intermediate states. Like in [21,22], our calculus works compositionally. It decomposes correctness statements about quantified hybrid programs structurally into corresponding statements about its parts by symbolic transformation.

Our approach combines the advantages of QdL in reasoning about the behaviour of operational distributed hybrid system models with those of TL to verify tempo-

ral statements about traces. We show that QdTL is sound and relatively complete. We argue that QdTL can verify practical systems and demonstrate this by studying temporal safety properties in distributed air traffic control. Our primary contributions are as follows:

- We introduce a logic for specifying and verifying temporal properties of distributed hybrid systems.
- We present a proof calculus for this logic, which, to the best of our knowledge, is the first verification approach that can handle temporal statements about distributed hybrid systems.
- We prove that this compositional calculus is a sound and complete axiomatization relative to differential equations.
- We verify temporal safety properties in a collision avoidance maneuver in distributed air traffic control, where aircraft can appear dynamically.

## 2 Related Work

Multi-party distributed control has been suggested for car control [15] and air traffic control [8]. Due to limits in verification technology, no formal analysis of temporal statements about the distributed hybrid dynamics has been possible for these systems yet. Analysis results include discrete message handling [15] or collision avoidance for two participants [8].

The importance of understanding dynamic/reconfigurable distributed hybrid systems was recognized in modeling languages SHIFT [7] and R-Charon [16]. They focused on simulation/compilation [7] or the development of a semantics [16], so that no verification is possible yet.

Other process-algebraic approaches, like  $\chi$  [27], have been developed for modeling and simulation. Verification is still limited to small fragments that can be translated directly to other verification tools like PHAVer or UPPAAL, which do not support distributed hybrid systems.

Our approach is completely different. It is based on first-order structures and dynamic logic. We focus on developing a logic that supports temporal and non-temporal statements about distributed hybrid dynamics and is amenable to automated theorem proving in the logic itself.

Our previous work and other verification approaches for static hybrid systems cannot verify distributed hybrid systems. Distributed hybrid systems may have an unbounded and changing number of components/participants, which cannot be represented with any fixed number of dimensions of the state space.

Based on [24], Beckert and Schlager [2] added separate trace modalities to dynamic logic and presented a relatively complete calculus. Their approach only handles discrete state spaces. In contrast, QdTL works for hybrid programs with continuous and structural/dimensional dynamics.

Davoren and Nerode [6] extended the propositional modal  $\mu$ -calculus with a semantics in hybrid systems and examine topological aspects. In [5], Davoren et al. gave a semantics in general flow systems for a generalisation of CTL\* [10]. In both cases, the authors of [6] and [5] provided Hilbert-style calculi to prove formulas that are valid for all systems simultaneously using abstract actions.

The strength of our logic primarily is that it is a first-order dynamic logic: it handles actual hybrid programs rather than only abstract actions of unknown effect. Our calculus directly supports verification of quantified hybrid programs with continuous evolution and structural/dimensional changes. First-order dynamic logic is more expressive and calculi are deductively stronger than other approaches [2,17].

### 3 Syntax of Quantified Differential Temporal Dynamic Logic

As a formal logic for verifying temporal specifications of distributed hybrid systems, we introduce *quantified differential temporal dynamic logic* (QdTL). QdTL extends dynamic logic for reasoning about system runs [12] with many-sorted first-order logic for reasoning about all ( $\forall i : A \phi$ ) or some ( $\exists i : A \phi$ ) objects of a sort  $A$ , e.g., the sort of all aircraft, and three other concepts:

*Quantified hybrid programs.* The behavior of distributed hybrid systems can be described by quantified hybrid programs [21,22], which generalize regular programs from dynamic logic [12] to distributed hybrid changes. The distinguish feature of quantified hybrid programs is that they provide uniform discrete transitions, continuous evolutions, and structural/dimension changes along quantified assignments and quantified differential equations, which can be combined by regular control operations.

*Modal operators.* Modalities of dynamic logic express statements about all possible behavior ( $[\alpha]\pi$ ) of a system  $\alpha$ , or about the existence of a trace ( $\langle\alpha\rangle\pi$ ), satisfying condition  $\pi$ . Unlike in standard dynamic logic,  $\alpha$  is a model of a distributed hybrid system. We use quantified hybrid programs to describe  $\alpha$  as in [21,22]. Yet, unlike in standard dynamic logic [12] or quantified differential dynamic logic (QdL) [21,22],  $\pi$  is a *trace formula* in QdTL, and  $\pi$  can refer to all states that occur *during* a trace using temporal operators.

*Temporal operators.* For QdTL, the temporal trace formula  $\Box\phi$  expresses that the formula  $\phi$  holds all along a trace selected by  $[\alpha]$  or  $\langle\alpha\rangle$ . For instance, the state formula  $\langle\alpha\rangle\Box\phi$  says that the state formula  $\phi$  holds at every state along at least one trace of  $\alpha$ . Dually, the trace formula  $\Diamond\phi$  expresses that  $\phi$  holds at some point during such a trace. It can occur in a state formula  $\langle\alpha\rangle\Diamond\phi$  to express that there is such a state in some trace of  $\alpha$ , or as  $[\alpha]\Diamond\phi$  to say that, along each trace, there is a state satisfying  $\phi$ . In this paper, the primary focus of attention is on homogeneous combinations of path and trace quantifiers like  $[\alpha]\Box\phi$  or  $\langle\alpha\rangle\Diamond\phi$ .

#### 3.1 Quantified Hybrid Programs

QdTL supports a (finite) number of object *sorts*, e.g., the sort of all aircraft, or the sort of all cars. For continuous quantities of distributed hybrid systems like positions or velocities, we add the sort  $\mathbb{R}$  for real numbers. *Terms* of QdTL are built from a set of (sorted) function/variable symbols as in many-sorted first-order logic. For representing appearance and disappearance of objects while running QHPs, we use an existence function symbol  $E(\cdot)$  that has value  $E(o) = 1$  if object  $o$  exists, and

has value  $E(o) = 0$  when object  $o$  disappears or has not been created yet. We use  $0, 1, +, -, \cdot$  with the usual notation and fixed semantics for real arithmetic. For  $n \geq 0$  we abbreviate  $f(s_1, \dots, s_n)$  by  $f(\mathbf{s})$  using vectorial notation and we use  $\mathbf{s} = \mathbf{t}$  for element-wise equality.

As a system model for distributed hybrid systems, QdTL uses *quantified hybrid programs* (QHP) [21,22]. The quantified hybrid programs occurring in dynamic modalities of QdTL are regular programs from dynamic logic [12] to which quantified assignments and quantified differential equation systems for distributed hybrid dynamics are added. QHPs are defined by the following grammar ( $\alpha, \beta$  are QHPs,  $\theta$  a term,  $i$  a variable of sort  $A$ ,  $f$  is a function symbol,  $\mathbf{s}$  is a vector of terms with sorts compatible to  $f$ , and  $\chi$  is a formula of first-order logic):

$$\alpha, \beta ::= \forall i : A \ f(\mathbf{s}) := \theta \mid \forall i : A \ f(\mathbf{s})' = \theta \ \& \ \chi \mid ?\chi \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

The effect of *quantified assignment*  $\forall i : A \ f(\mathbf{s}) := \theta$  is an instantaneous discrete jump assigning  $\theta$  to  $f(\mathbf{s})$  simultaneously for all objects  $i$  of sort  $A$ . The QHP  $\forall i : C \ a(i) := a(i) + 1$ , for example, expresses that all cars  $i$  of sort  $C$  simultaneously increase their acceleration  $a(i)$ . The effect of *quantified differential equation*  $\forall i : A \ f(\mathbf{s})' = \theta \ \& \ \chi$  is a continuous evolution where, for all objects  $i$  of sort  $A$ , all differential equations  $f(\mathbf{s})' = \theta$  hold and formula  $\chi$  holds throughout the evolution (the state remains in the region described by  $\chi$ ). The dynamics of QHPs changes the interpretation of terms over time:  $f(\mathbf{s})'$  is intended to denote the derivative of the interpretation of the term  $f(\mathbf{s})$  over time during continuous evolution, not the derivative of  $f(\mathbf{s})$  by its argument  $\mathbf{s}$ . For  $f(\mathbf{s})'$  to be defined, we assume  $f$  is an  $\mathbb{R}$ -valued function symbol. For simplicity, we assume that  $f$  does not occur in  $\mathbf{s}$ . In most quantified assignments/differential equations  $\mathbf{s}$  is just  $i$ . For instance, the following QHP expresses that all cars  $i$  of sort  $C$  drive by  $\forall i : C \ x(i)'' = a(i)$  such that their position  $x(i)$  changes continuously according to their respective acceleration  $a(i)$ .

The effect of test  $?\chi$  is a *skip* (i.e., no change) if formula  $\chi$  is true in the current state and *abort* (blocking the system run by a failed assertion), otherwise. *Nondeterministic choice*  $\alpha \cup \beta$  is for alternatives in the behavior of the distributed hybrid system. In the *sequential composition*  $\alpha; \beta$ , QHP  $\beta$  starts after  $\alpha$  finishes ( $\beta$  never starts if  $\alpha$  continues indefinitely). *Nondeterministic repetition*  $\alpha^*$  repeats  $\alpha$  an arbitrary number of times, possibly zero times.

Structural dynamics of distributed hybrid systems corresponds to quantified assignments to function terms and we model the appearance of new participants in the distributed hybrid system, e.g., new aircraft appearing into the local flight scenario, by a program  $n := \text{new } A$  (see [21,22] for details).

### 3.2 State and Trace Formulas

The formulas of QdTL are defined similarly to first-order dynamic logic plus many-sorted first-order logic. However, the modalities  $[\alpha]$  and  $\langle \alpha \rangle$  accept trace formulas that refer to the temporal behavior of *all* states along a trace. Inspired by CTL and CTL\* [9,10], we distinguish between state formulas, which are true or false in states, and trace formulas, which are true or false for system traces.

The *state formulas* of QdTL are defined by the following grammar ( $\phi, \psi$  are state formulas,  $\pi$  is a trace formula,  $\theta_1, \theta_2$  are terms of the same sort,  $i$  is a variable of sort  $A$ , and  $\alpha$  is a QHP):

$$\phi, \psi ::= \theta_1 = \theta_2 \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall i : A \phi \mid \exists i : A \phi \mid [\alpha]\pi \mid \langle \alpha \rangle \pi$$

We use standard abbreviations to define  $\leq, >, <, \vee, \rightarrow$ . Sorts  $A \neq \mathbb{R}$  have no ordering and only  $\theta_1 = \theta_2$  is allowed. For sort  $\mathbb{R}$ , we abbreviate  $\forall x : \mathbb{R} \phi$  by  $\forall x \phi$ .

The *trace formulas* of QdTL are defined by the following grammar ( $\pi$  is a trace formula and  $\phi$  is a state formula):

$$\pi ::= \phi \mid \Box\phi \mid \Diamond\phi$$

Formulas without  $\Box$  and  $\Diamond$  are *non-temporal QdL formulas*. Unlike in CTL, state formulas are true on a trace if they hold for the *last* state of a trace, not for the first. Thus,  $[\alpha]\phi$  expresses that  $\phi$  is true at the end of each trace of  $\alpha$ . In contrast,  $[\alpha]\Box\phi$  expresses that  $\phi$  is true all along all states of every trace of  $\alpha$ . This combination gives a smooth embedding of non-temporal QdL into QdTL and makes it possible to define a compositional calculus. Like CTL, QdTL allows nesting with a branching time semantics [9], e.g.,  $[\alpha]\Box((\forall i : C \ x(i) \geq 2) \rightarrow \langle \beta \rangle \Diamond(\forall i : C \ x(i) \leq 0))$ . In the following, all formulas and terms have to be well-typed. For short notation, we allow conditional terms of the form *if  $\phi$  then  $\theta_1$  else  $\theta_2$  fi* (where  $\theta_1$  and  $\theta_2$  have the same sort). This term evaluates to  $\theta_1$  if the formula  $\phi$  is true and to  $\theta_2$  otherwise. We consider formulas with conditional terms as abbreviations, e.g.,  $\psi(\text{if } \phi \text{ then } \theta_1 \text{ else } \theta_2)$  for  $(\phi \rightarrow \psi(\theta_1)) \wedge (\neg\phi \rightarrow \psi(\theta_2))$ .

*Example 1.* Let  $C$  be the sort of all cars. By  $x(i)$ , we denote the position of car  $i$ , by  $v(i)$  its velocity and by  $a(i)$  its acceleration. Then the QdTL formula

$$(\forall i : C \ x(i) \geq 0) \rightarrow [\forall i : C \ x(i)' = v(i), v(i)' = a(i) \ \& \ v(i) \geq 0] \Box (\forall i : C \ x(i) \geq 0)$$

says that, if all cars start at a point to the right of the origin and we only allow them to evolve as long as all of them have nonnegative velocity, then they *always* stay up to the right of the origin. In this case, the QHP just consists of a quantified differential equation expressing that the position  $x(i)$  of car  $i$  evolves over time according to the velocity  $v(i)$ , which evolves according to its acceleration  $a(i)$ . The constraint  $v(i) \geq 0$  expresses that the cars never move backwards, which otherwise would happen eventually in the case of braking  $a(i) < 0$ . This formula is indeed valid, and we would be able to use the techniques developed in this paper to prove it.

## 4 Semantics of Quantified Differential Temporal Dynamic Logic

In standard dynamic logic [12] and the logic QdL [21,22], modalities only refer to the final states of system runs and the semantics is a reachability relation on states: State  $\tau$  is reachable from state  $\sigma$  using  $\alpha$  if there is a run of  $\alpha$  which terminates in  $\tau$  when started in  $\sigma$ . For QdTL, however, formulas can refer to intermediate states of runs as well. Thus, the semantics of a distributed hybrid system  $\alpha$  is the set of its possible *traces*, i.e., successions of states that occur during the evolution of  $\alpha$ .

#### 4.1 Trace Semantics of Quantified Hybrid Programs

A *state*  $\sigma$  associates an infinite set  $\sigma(A)$  of objects with each sort  $A$ , and it associates a function  $\sigma(f)$  of appropriate type with each function symbol  $f$ , including  $E(\cdot)$ . For simplicity,  $\sigma$  also associates a value  $\sigma(i)$  of appropriate type with each variable  $i$ . The domain of  $\mathbb{R}$  and the interpretation of  $0, 1, +, -, \cdot$  is that of real arithmetic. We assume constant domain for each sort  $A$ : all states  $\sigma, \tau$  share the same infinite domains  $\sigma(A) = \tau(A)$ . Sorts  $A \neq C$  are disjoint:  $\sigma(A) \cap \sigma(C) = \emptyset$ . The set of all states is denoted by  $\mathcal{S}$ . The state  $\sigma_i^e$  agrees with  $\sigma$  except for the interpretation of variable  $i$ , which is changed to  $e$ . In addition, we distinguish a state  $\Lambda$  to denote the failure of a system run when it is *aborted* due to a test  $? \chi$  that yields *false*. In particular,  $\Lambda$  can only occur at the end of an aborted system run and marks that there is no further extension.

Distributed hybrid systems evolve along piecewise continuous traces in multi-dimensional space, structural changes, and appearance or disappearance of agents as time passes. Continuous phases are governed by differential equations, whereas discontinuities are caused by discrete jumps. Unlike in discrete cases [2,24], traces are not just sequences of states, since distributed hybrid systems pass through uncountably many states even in bounded time. Beyond that, continuous changes are more involved than in pure real-time [1,14], because all variables can evolve along different differential equations. Generalizing the real-time traces of [14], the following definition captures hybrid behavior by splitting the uncountable succession of states into periods  $\nu_i$  that are regulated by the same control law. For discrete jumps, some periods are point flows of duration 0.

The (trace) semantics of quantified hybrid programs is compositional, that is, the semantics of a complex program is defined as a simple function of the trace semantics of its parts.

**Definition 1 (Hybrid Trace).** *A trace is a (non-empty) finite or infinite sequence  $\nu = (\nu_0, \nu_1, \nu_2, \dots)$  of functions  $\nu_k : [0, r_k] \rightarrow \mathcal{S}$  with respective durations  $r_k \in \mathbb{R}$  (for  $k \in \mathbb{N}$ ). A position of  $\nu$  is a pair  $(k, \zeta)$  with  $k \in \mathbb{N}$  and  $\zeta$  in the interval  $[0, r_k]$ ; the state of  $\nu$  at  $(k, \zeta)$  is  $\nu_k(\zeta)$ . Positions of  $\nu$  are ordered lexicographically by  $(k, \zeta) \prec (m, \xi)$  iff either  $k < m$ , or  $k = m$  and  $\zeta < \xi$ . Further, for a state  $\sigma \in \mathcal{S}$ ,  $\hat{\sigma} : 0 \mapsto \sigma$  is the point flow at  $\sigma$  with duration 0. A trace terminates if it is a finite sequence  $(\nu_0, \nu_1, \dots, \nu_n)$  and  $\nu_n(r_n) \neq \Lambda$ . In that case, the last state  $\nu_n(r_n)$  is denoted by  $\text{last } \nu$ . The first state  $\nu_0(0)$  is denoted by  $\text{first } \nu$ .*

Unlike in [1,14], the definition of traces also admits finite traces of bounded duration, which is necessary for compositionality of traces in  $\alpha; \beta$ . The semantics of quantified hybrid programs  $\alpha$  as the set  $\mu(\alpha)$  of its possible traces depends on valuations  $\sigma[\![\cdot]\!]$  of formulas and terms at intermediate states  $\sigma$ . The valuation of formulas will be defined in Definition 3. Especially, we use  $\sigma_i^e[\![\cdot]\!]$  to denote the valuations of terms and formulas in state  $\sigma_i^e$ , i.e., in state  $\sigma$  with  $i$  interpreted as  $e$ .

**Definition 2 (Trace Semantics of Quantified Hybrid Programs).** *The trace semantics,  $\mu(\alpha)$ , of a quantified hybrid program  $\alpha$ , is the set of all its possible hybrid traces and is defined inductively as follows:*

1.  $\mu(\forall i : A \ f(\mathbf{s}) := \theta) = \{(\hat{\sigma}, \hat{\tau}) : \sigma \in \mathcal{S} \text{ and state } \tau \text{ is identical to } \sigma \text{ except that at each position } \mathbf{o} \text{ of } f: \text{ if } \sigma_i^e[\mathbf{s}] = \mathbf{o} \text{ for some object } e \in \sigma(A), \text{ then } \tau(f)(\sigma_i^e[\mathbf{s}]) = \sigma_i^e[\theta].\}$
2.  $\mu(\forall i : A \ f(\mathbf{s})' = \theta \ \& \ \chi) = \{(\varphi) : 0 \leq r \in \mathbb{R} \text{ and } \varphi : [0, r] \rightarrow \mathcal{S} \text{ is a function satisfying the following conditions. At each time } t \in [0, r], \text{ state } \varphi(t) \text{ is identical to } \varphi(0), \text{ except that at each position } \mathbf{o} \text{ of } f : \text{ if } \sigma_i^e[\mathbf{s}] = \mathbf{o} \text{ for some object } e \in \sigma(A), \text{ then, at each time } \zeta \in [0, r]:$   
 – The differential equations hold and derivatives exist (trivial for  $r = 0$ ):

$$\frac{d(\varphi(t)_i^e[f(\mathbf{s})])}{dt}(\zeta) = (\varphi(\zeta)_i^e[\theta])$$

- The evolution domains is respected:  $\varphi(\zeta)_i^e[\chi] = \text{true}$ .
3.  $\mu(? \chi) = \{(\hat{\sigma}) : \sigma[\chi] = \text{true}\} \cup \{(\hat{\sigma}, \hat{A}) : \sigma[\chi] = \text{false}\}$
4.  $\mu(\alpha \cup \beta) = \mu(\alpha) \cup \mu(\beta)$
5.  $\mu(\alpha; \beta) = \{\nu \circ \varsigma : \nu \in \mu(\alpha), \varsigma \in \mu(\beta) \text{ when } \nu \circ \varsigma \text{ is defined}\}$ ; the composition of  $\nu = (\nu_0, \nu_1, \nu_2, \dots)$  and  $\varsigma = (\varsigma_0, \varsigma_1, \varsigma_2, \dots)$  is
 
$$\nu \circ \varsigma = \begin{cases} (\nu_0, \dots, \nu_n, \varsigma_0, \varsigma_1, \dots) & \text{if } \nu \text{ terminates at } \nu_n \text{ and last } \nu = \text{first } \varsigma \\ \nu & \text{if } \nu \text{ does not terminate} \\ \text{not defined} & \text{otherwise} \end{cases}$$
6.  $\mu(\alpha^*) = \bigcup_{n \in \mathbb{N}} \mu(\alpha^n)$ , where  $\alpha^{n+1} := (\alpha^n; \alpha)$  for  $n \geq 1$ , as well as  $\alpha^1 := \alpha$  and  $\alpha^0 := (? \text{true})$ .

## 4.2 Valuation of State and Trace Formulas

**Definition 3 (Valuation of Formulas).** The valuation of state and trace formulas is defined respectively. For state formulas, the valuation  $\sigma[\cdot]$  with respect to state  $\sigma$  is defined as follows:

1.  $\sigma[\theta_1 = \theta_2] = \text{true}$  iff  $\sigma[\theta_1] = \sigma[\theta_2]$ ; accordingly for  $\geq$ .
2.  $\sigma[\phi \wedge \psi] = \text{true}$  iff  $\sigma[\phi] = \text{true}$  and  $\sigma[\psi] = \text{true}$ ; accordingly for  $\neg$ .
3.  $\sigma[\forall i : A \ \phi] = \text{true}$  iff  $\sigma_i^e[\phi] = \text{true}$  for all objects  $e \in \sigma(A)$ .
4.  $\sigma[\exists i : A \ \phi] = \text{true}$  iff  $\sigma_i^e[\phi] = \text{true}$  for some object  $e \in \sigma(A)$ .
5.  $\sigma[[\alpha]\pi] = \text{true}$  iff for each trace  $\nu \in \mu(\alpha)$  that starts in  $\text{first } \nu = \sigma$ , if  $\nu[\pi]$  is defined, then  $\nu[\pi] = \text{true}$ .
6.  $\sigma[\langle \alpha \rangle \pi] = \text{true}$  iff there is a trace  $\nu \in \mu(\alpha)$  starting in  $\text{first } \nu = \sigma$  such that  $\nu[\pi]$  is defined and  $\nu[\pi] = \text{true}$ .

For trace formulas, the valuation  $\nu[\cdot]$  with respect to trace  $\nu$  is defined as follows:

1. If  $\phi$  is a state formula, then  $\nu[\phi] = \text{last } \nu[\phi]$  if  $\nu$  terminates, whereas  $\nu[\phi]$  is not defined if  $\nu$  does not terminate.
2.  $\nu[\Box \phi] = \text{true}$  iff  $\nu_k(\zeta)[\phi] = \text{true}$  for all positions  $(k, \zeta)$  of  $\nu$  with  $\nu_k(\zeta) \neq \Lambda$ .
3.  $\nu[\Diamond \phi] = \text{true}$  iff  $\nu_k(\zeta)[\phi] = \text{true}$  for some position  $(k, \zeta)$  of  $\nu$  with  $\nu_k(\zeta) \neq \Lambda$ .

As usual, a (state) formula is *valid* if it is true in all states. Further for (state) formula  $\phi$  and state  $\sigma$  we write  $\sigma \models \phi$  iff  $\sigma[\phi] = \text{true}$ . We write  $\sigma \not\models \phi$  iff  $\sigma[\phi] = \text{false}$ . Likewise, for trace formula  $\pi$  and trace  $\nu$  we write  $\nu \models \pi$  iff  $\nu[\pi] = \text{true}$  and  $\nu \not\models \pi$  iff  $\nu[\pi] = \text{false}$ . In particular, we only write  $\nu \models \pi$  or  $\nu \not\models \pi$  if  $\nu[\pi]$  is defined, which it is not the case if  $\pi$  is a state formula and  $\nu$  does not terminate.



### 4.3 Conservative Temporal Extension

The following result shows that the extension of QdTL by temporal operators does not change the meaning of non-temporal Qd $\mathcal{L}$  formulas. The trace semantics given in Definition 3 is equivalent to the final state reachability relation semantics [21,22] for the sublogic Qd $\mathcal{L}$  of QdTL.

**Proposition 1.** *The logic QdTL is a conservative extension of non-temporal Qd $\mathcal{L}$ , i.e., the set of valid Qd $\mathcal{L}$  formulas is the same with respect to transition reachability semantics of Qd $\mathcal{L}$  [21,22] as with respect to the trace semantics of QdTL (Definition 3).*

## 5 Safety Properties in Distributed Air Traffic Control

In air traffic control, collision avoidance maneuvers [8,26] are used to resolve conflicting flight paths that arise during free flight. We consider the roundabout collision avoidance maneuver for air traffic control [26]. In the literature, formal verification of the hybrid dynamics of air traffic control focused on a fixed number of aircraft, usually two. In reality, many more aircraft are in the same flight corridor, even if not all of them participate in the same maneuver. They may be involved in multiple distributed maneuvers at the same time, however. Perfect global trajectory planning quickly becomes infeasible then. The verification itself also becomes much more complicated for three aircraft already. Explicit replication of the system dynamics  $n$  times is computationally infeasible for larger  $n$ . Yet, collision avoidance maneuvers need to work for an (essentially) unbounded number of aircraft. Because global trajectory planning is infeasible, the appearance of other aircraft into a local collision avoidance maneuver always has to be expected and managed safely. See Fig. 1 for a general illustration of roundabout-style collision avoidance maneuvers and the phenomenon of dynamic appearance of some new aircraft  $z$  into the horizon of relevance.

The resulting flight control system has several characteristics of hybrid dynamics. But it is not a hybrid system and does not even have a fixed finite number of variables in a fixed finite-dimensional state space. The system forms a distributed hybrid system, in which all aircraft fly at the same time and new aircraft may appear from remote areas into the local flight scenario. Let  $A$  be the sort of all aircraft. Each aircraft  $i$  has a position  $x(i) = (x_1(i), x_2(i))$  and a velocity vector  $d(i) = (d_1(i), d_2(i))$ . We model the continuous dynamics of an aircraft  $i$  that follows a flight curve with an angular velocity  $\omega(i)$  by the (function) differential equation:

$$x_1(i)' = d_1(i), x_2(i)' = d_2(i), d_1(i)' = -\omega(i)d_2(i), d_2(i)' = \omega(i)d_1(i) \quad (\mathcal{F}_{\omega(i)}(i))$$

This differential equation, which we denote by  $\mathcal{F}_{\omega(i)}(i)$ , is the standard equation for curved flight from the literature [26], but lifted to function symbols that are

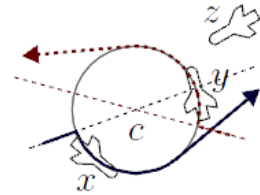


Fig. 1: Roundabout collision avoidance maneuver with new appearance

parameterized by aircraft  $i$ . Now the quantified differential equation  $\forall i : A \mathcal{F}_{\omega(i)}(i)$  characterizes that *all* aircraft  $i$  fly along their respective (function) differential equation  $\mathcal{F}_{\omega(i)}(i)$  according to their respective angular velocities  $\omega(i)$  at the same time. This quantified differential equation captures what no finite-dimensional differential equation system could ever do. It characterizes the simultaneous movement of an unbounded, arbitrary, and even growing or shrinking set of aircraft.

Two aircraft  $i$  and  $j$  have violated the safe separation property if they falsify the following formula

$$\mathcal{P}(i, j) \equiv i = j \vee (x_1(i) - x_1(j))^2 + (x_2(i) - x_2(j))^2 \geq p^2$$

which says that aircraft  $i$  and  $j$  are either identical or separated by at least the protected zone  $p$  (usually 5mi). For the aircraft control system to be safe, all aircraft have to be safely separated, i.e., need to satisfy  $\forall i, j : A \mathcal{P}(i, j)$ . It is crucial that this formula holds at *every* point in time during the system evolution, not only at its beginning or at its end. Hence, we need to consider temporal safety properties. For instance, QdTL can analyze the following temporal safety properties of a part of the distributed roundabout collision avoidance maneuver for air traffic control:

$$\forall i, j : A \mathcal{P}(i, j) \wedge \forall i, j : A \mathcal{T}(i, j) \rightarrow [\forall i : A \mathcal{F}_{\omega(i)}(i)] \Box \forall i, j : A \mathcal{P}(i, j) \quad (1)$$

$$\begin{aligned} & \forall i, j : A \mathcal{P}(i, j) \wedge \forall i, j : A \mathcal{T}(i, j) \rightarrow \\ & [\forall i : A t := 0; \forall i : A \mathcal{F}_{\omega(i)}(i), t' = 1 \ \& \ \forall i : A t \leq T; ?(\forall i : A t = T)] \Box \forall i, j : A \mathcal{P}(i, j) \end{aligned} \quad (2)$$

where  $\mathcal{T}(i, j) \equiv d_1(i) - d_1(j) = -\omega(x_2(i) - x_2(j)) \wedge d_2(i) - d_2(j) = \omega(x_1(i) - x_1(j))$ ,  $t$  is a clock variable, and  $T$  is some bounded time.

The temporal safety invariant in (1) expresses that the circle phase of roundabout maneuver *always* stays collision-free indefinitely for an arbitrary number of aircraft. That is the most crucial part because we have to know the aircraft *always* remain safe during the actual roundabout collision avoidance circle. The condition  $\forall i, j : A \mathcal{T}(i, j)$  characterizes compatible tangential maneuvering choices. Without a condition like  $\mathcal{T}(i, j)$ , roundabouts can be unsafe [20]. For a systematic derivation of how to construct  $\mathcal{T}(i, j)$ , we refer to the work [20]. As a variation of (1), the temporal safety property in (2) states that, for an arbitrary number of aircraft, the circle procedure of roundabout maneuver cannot produce collisions at any point in its bounded duration  $T$ . This variation restricts the continuous evolution to take exactly  $T$  time units (the evolution domain region restricts the evolution to  $t \leq T$  and the subsequent test to  $?( \forall i : A t = T )$ ) and no intermediate state is visible as a final state anymore. Thus, the temporal modality  $\Box$  in (2) is truly necessary. We will use the techniques developed in this paper to verify these temporal safety properties in the distributed roundabout flight collision avoidance maneuver.

## 6 Proof Calculus for Temporal Properties

In this section, we introduce a sequent calculus for verifying temporal specifications of distributed hybrid systems in QdTL. With the basic idea being to perform

a symbolic decomposition, the calculus transforms quantified hybrid programs successively into simpler logical formulas describing their effects. Statements about the temporal behavior of a quantified hybrid program are successively reduced to corresponding non-temporal statements about the intermediate states.

## 6.1 Proof Rules

In Fig. 2, we present a proof calculus for QdTL that inherits the proof rules of QdL from [21,22] and adds new proof rules for temporal modalities. We use the sequent notation informally for a systematic proof structure. A *sequent* is of the form  $\Gamma \rightarrow \Delta$ , where the *antecedent*  $\Gamma$  and *succedent*  $\Delta$  are finite sets of formulas. The semantics of  $\Gamma \rightarrow \Delta$  is that of the formula  $\bigwedge_{\phi \in \Gamma} \phi \rightarrow \bigvee_{\psi \in \Delta} \psi$  and will be treated as an abbreviation. As usual in sequent calculus, the proof rules are applied backwards from the *conclusion* (goal below horizontal bar) to the *premises* (subgoals above bar).

**Inherited Non-temporal Rules** The QdTL calculus inherits the (non-temporal) QdL proof rules. For propositional logic, standard rules *ax-cut* are listed in Fig. 2. Rules  $[-](?)$  work similar to those in [12]. Rules  $[']$ ,  $\langle '\rangle$  handle continuous evolutions for quantified differential equations with first-order definable solutions. Rules  $[:=]-\langle :*\rangle$  handle discrete changes for quantified assignments. Axiom *ex* expresses that, for sort  $A \neq \mathbb{R}$ , there always is a new object  $n$  that has not been created yet ( $E(n) = 0$ ), because domains are infinite. The quantifier rules  $\forall r-i\exists$  combine quantifier handling of many-sorted logic based on instantiation with theory reasoning by *quantifier elimination* (QE) for the theory of reals. The global rules  $\llbracket gen$ ,  $\langle \rangle gen$  are Gödel generalization rules and *ind* is an induction schema for loops with *inductive invariant*  $\phi$  [12]. Similarly, *con* generalizes Harel’s convergence rule [12] to the hybrid case with decreasing variant  $\varphi$  [19]. *DI* and *DC* are rules for quantified differential equations with *quantified differential invariants* [21,22]. Notice that  $[\cup]$ ,  $\langle \cup \rangle$  can be generalized to apply to formulas of the form  $[\alpha \cup \beta]\pi$  where  $\pi$  is an arbitrary trace formula, and not just a state formula as in QdL. Thus,  $\pi$  may begin with  $\Box$  and  $\Diamond$ , which is why the rules are repeated in this generalized form as  $[\cup]\Box$  and  $\langle \cup \rangle \Diamond$  in Fig. 2.

**Temporal Rules** The new temporal rules in Fig. 2 for the QdTL calculus successively transform temporal specifications of quantified hybrid programs into non-temporal QdL formulas. The idea underlying this transformation is to decompose quantified hybrid programs and recursively augment intermediate state transitions with appropriate specifications.

Rule  $[-]\Box$  decomposes invariants of  $\alpha;\beta$  (i.e.,  $[\alpha;\beta]\Box\phi$  holds) into an invariant of  $\alpha$  (i.e.,  $[\alpha]\Box\phi$ ) and an invariant of  $\beta$  that holds when  $\beta$  is started in *any* final state of  $\alpha$  (i.e.,  $[\alpha](\Box\phi)$ ). Its difference with the QdL rule  $[-]$  thus is that the QdTL rule  $[-]\Box$  also checks safety invariant  $\phi$  at the symbolic states in between the execution of  $\alpha$  and  $\beta$ , and recursively so because of the temporal modality  $\Box$ . Rule  $[:=]\Box$  expresses that invariants of quantified assignments need to hold before and after the discrete change (similarly for  $[?]\Box$ , except that tests do not lead to a state change, so  $\phi$  holding before the test is all there is to it). Rule  $[']\Box$  can directly

$$\begin{array}{l}
(ax) \frac{}{\phi \rightarrow \phi} \quad (\neg r) \frac{\phi \rightarrow}{\neg \phi} \quad (\neg l) \frac{\rightarrow \phi}{\neg \phi \rightarrow} \quad (\wedge r) \frac{\rightarrow \phi \quad \rightarrow \psi}{\rightarrow \phi \wedge \psi} \quad (\wedge l) \frac{\phi, \psi \rightarrow}{\phi \wedge \psi \rightarrow} \quad (cut) \frac{\rightarrow \phi \quad \phi \rightarrow}{\rightarrow} \\
([;]) \frac{[\alpha][\beta]\phi \quad (\langle; \rangle)}{[\alpha; \beta]\phi} \quad (\langle; \rangle) \frac{\langle \alpha \rangle \langle \beta \rangle \phi}{\langle \alpha; \beta \rangle \phi} \quad ([\cup]) \frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi} \quad (\langle \cup \rangle) \frac{\langle \alpha \rangle \phi \vee \langle \beta \rangle \phi}{\langle \alpha \cup \beta \rangle \phi} \quad ([?]) \frac{\chi \rightarrow \phi}{[?]\chi} \quad (\langle ? \rangle) \frac{\chi \wedge \phi}{\langle ? \rangle \chi} \\
([']) \frac{\forall t \geq 0 ((\forall 0 \leq \tilde{t} \leq t [\forall i : A \mathcal{S}(\tilde{t})] \chi) \rightarrow [\forall i : A \mathcal{S}(t)] \phi)}{[\forall i : A f(\mathbf{s})' = \theta \& \chi] \phi} \quad 1 \quad (\langle' \rangle) \frac{\exists t \geq 0 ((\forall 0 \leq \tilde{t} \leq t [\forall i : A \mathcal{S}(\tilde{t})] \chi) \wedge \langle \forall i : A \mathcal{S}(t) \rangle \phi)}{\langle \forall i : A f(\mathbf{s})' = \theta \& \chi \rangle \phi} \\
([:=]) \frac{\text{if } \exists i : A \mathbf{s} = [\mathcal{A}]\mathbf{u} \text{ then } \forall i : A (\mathbf{s} = [\mathcal{A}]\mathbf{u} \rightarrow \phi(\theta)) \text{ else } \phi(f([\mathcal{A}]\mathbf{u})) \text{ fi}}{\phi([\forall i : A f(\mathbf{s}) := \theta]f(\mathbf{u}))} \quad 2 \\
([:=]) \frac{\text{if } \exists i : A \mathbf{s} = \langle \mathcal{A} \rangle \mathbf{u} \text{ then } \exists i : A (\mathbf{s} = \langle \mathcal{A} \rangle \mathbf{u} \wedge \phi(\theta)) \text{ else } \phi(f(\langle \mathcal{A} \rangle \mathbf{u})) \text{ fi}}{\phi(\langle \forall i : A f(\mathbf{s}) := \theta \rangle f(\mathbf{u}))} \quad 2 \\
(skip) \frac{\Upsilon([\forall i : A f(\mathbf{s}) := \theta]\mathbf{u})}{[\forall i : A f(\mathbf{s}) := \theta]\Upsilon(\mathbf{u})} \quad 3 \quad ([; *]) \frac{\forall j : A \phi(\theta)}{[\forall j : A n := \theta]\phi(n)} \quad (\langle; * \rangle) \frac{\exists j : A \phi(\theta)}{\langle \forall j : A n := \theta \rangle \phi(n)} \quad (ex) \frac{true}{\exists n : A E(n) = 0} \\
(\forall r) \frac{\Gamma \rightarrow \phi(f(X_1, \dots, X_n)), \Delta}{\Gamma \rightarrow \forall x \phi(x), \Delta} \quad 4 \quad (\exists r) \frac{\Gamma \rightarrow \phi(\theta), \exists x \phi(x), \Delta}{\Gamma \rightarrow \exists x \phi(x), \Delta} \quad 5 \quad (\forall l) \frac{\Gamma, \phi(\theta), \forall x \phi(x) \rightarrow \Delta}{\Gamma, \forall x \phi(x) \rightarrow \Delta} \quad 5 \quad (\exists l) \frac{\Gamma, \phi(f(X_1, \dots, X_n)) \rightarrow \Delta}{\Gamma, \exists x \phi(x) \rightarrow \Delta} \\
(i\forall) \frac{QE(\forall X, Y (\text{if } \mathbf{s} = \mathbf{t} \text{ then } \Phi(X) \rightarrow \Psi(X) \text{ else } \Phi(X) \rightarrow \Psi(Y) \text{ fi}))}{\Phi(f(\mathbf{s})) \rightarrow \Psi(f(\mathbf{t}))} \quad 6 \quad (i\exists) \frac{QE(\exists X \bigwedge_i (\Phi_i \rightarrow \Psi_i))}{\Phi_1 \rightarrow \Psi_1 \dots \Phi_n \rightarrow \Psi_n} \quad 7 \\
([gen]) \frac{\phi \rightarrow \psi}{\Gamma, [\alpha]\phi \rightarrow [\alpha]\psi, \Delta} \quad (\langle gen \rangle) \frac{\phi \rightarrow \psi}{\Gamma, \langle \alpha \rangle \phi \rightarrow \langle \alpha \rangle \psi, \Delta} \quad (ind) \frac{\phi \rightarrow [\alpha]\phi}{\Gamma, \phi \rightarrow [\alpha^*]\phi, \Delta} \quad (con) \frac{v > 0 \wedge \varphi(v) \rightarrow \langle \alpha \rangle \varphi(v-1)}{\Gamma, \exists v \varphi(v) \rightarrow \langle \alpha^* \rangle \exists v \leq 0 \varphi(v), \Delta} \quad 8 \\
(DI) \frac{\chi \rightarrow [\forall i : A f(\mathbf{s})' := \theta]D(\phi)}{\phi \rightarrow [\forall i : A f(\mathbf{s})' = \theta \& \chi] \phi} \quad 9 \quad (DC) \frac{\phi \rightarrow [\forall i : A f(\mathbf{s})' = \theta \& \chi] \psi \quad \phi \rightarrow [\forall i : A f(\mathbf{s})' = \theta \& \chi] \phi}{\phi \rightarrow [\forall i : A f(\mathbf{s})' = \theta \& \chi] \phi} \\
([\cup]) \frac{[\alpha]\pi \wedge [\beta]\pi}{[\alpha \cup \beta]\pi} \quad 10 \quad (\langle \cup \rangle) \frac{\langle \alpha \rangle \pi \vee \langle \beta \rangle \pi}{\langle \alpha \cup \beta \rangle \pi} \quad ([; \square]) \frac{[\alpha]\square\phi \wedge [\beta]\square\phi}{[\alpha; \beta]\square\phi} \quad (\langle; \rangle \diamond) \frac{\langle \alpha \rangle \diamond \phi \vee \langle \beta \rangle \diamond \phi}{\langle \alpha; \beta \rangle \diamond \phi} \\
([?]\square) \frac{\phi}{[\chi]\square\phi} \quad (\langle ? \rangle \diamond) \frac{\phi}{\langle \chi \rangle \diamond \phi} \\
([:=]\square) \frac{\phi \wedge [\forall i : A f(\mathbf{s}) := \theta] \phi}{[\forall i : A f(\mathbf{s}) := \theta] \square \phi} \quad (\langle := \rangle \diamond) \frac{\phi \vee \langle \forall i : A f(\mathbf{s}) := \theta \rangle \phi}{\langle \forall i : A f(\mathbf{s}) := \theta \rangle \diamond \phi} \\
([']\square) \frac{[\forall i : A f(\mathbf{s})' = \theta \& \chi] \phi}{[\forall i : A f(\mathbf{s})' = \theta \& \chi] \square \phi} \quad (\langle' \rangle \diamond) \frac{\langle \forall i : A f(\mathbf{s})' = \theta \& \chi \rangle \phi}{\langle \forall i : A f(\mathbf{s})' = \theta \& \chi \rangle \diamond \phi} \\
([*n]\square) \frac{[\alpha; \alpha^*]\square\phi}{[\alpha^*]\square\phi} \quad (\langle *n \rangle \diamond) \frac{\langle \alpha; \alpha^* \rangle \diamond \phi}{\langle \alpha^* \rangle \diamond \phi} \quad ([*]\square) \frac{[\alpha^*]\square\phi}{[\alpha^*]\square\phi} \quad (\langle * \rangle \diamond) \frac{\langle \alpha^* \rangle \langle \alpha \rangle \diamond \phi}{\langle \alpha^* \rangle \diamond \phi}
\end{array}$$

- <sup>1</sup>  $t, \tilde{t}$  are new variables,  $\forall i : A \mathcal{S}(t)$  is the quantified assignment  $\forall i : A f(\mathbf{s}) := y_s(t)$  with solutions  $y_s(t)$  of the (injective) differential equations and  $f(\mathbf{s})$  as initial values. See [21,22] for the definition of a *injective* quantified assignment or quantified differential equation.
- <sup>2</sup> Occurrence  $f(\mathbf{u})$  in  $\phi(f(\mathbf{u}))$  is not in scope of a modality (admissible substitution) and we abbreviate assignment  $\forall i : A f(\mathbf{s}) := \theta$  by  $\mathcal{A}$ , which is assumed to be injective.
- <sup>3</sup>  $f \neq \Upsilon$  and the quantified assignment  $\forall i : A f(\mathbf{s}) := \theta$  is injective. The same rule applies for  $\langle \forall i : A f(\mathbf{s}) := \theta \rangle$  instead of  $[\forall i : A f(\mathbf{s}) := \theta]$ .
- <sup>4</sup>  $f$  is a new (Skolem) function and  $X_1, \dots, X_n$  are all free logical variables of  $\forall x \phi(x)$ .
- <sup>5</sup>  $\theta$  is an abbreviate term, often a new logical variable.
- <sup>6</sup>  $X, Y$  are new variables of sort  $\mathbb{R}$ . QE needs to be applicable in the premises.
- <sup>7</sup> Among all open branches, the free (existential) logical variable  $X$  of sort  $\mathbb{R}$  only occurs in the branch  $\Phi_i \rightarrow \Psi_i$ . QE needs to be defined for the formula in the premises, especially, no Skolem dependencies on  $X$  occur.
- <sup>8</sup> logical variable  $v$  does not occur in  $\alpha$ .
- <sup>9</sup> The operator  $D$ , as defined in [21,22], is used to computer syntactic total derivations of formulas algebraically.
- <sup>10</sup>  $\pi$  is a trace formula, whereas  $\phi$  and  $\psi$  are (state) formulas. Unlike  $\phi$  and  $\psi$ , the trace formula  $\pi$  may thus begin with a temporal modality  $\square$  or  $\diamond$ .

Fig. 2: Rule schemata of the proof calculus for quantified differential temporal dynamic logic

reduce invariants of continuous evolutions to non-temporal formulas as restrictions of solutions of quantified differential equations are themselves solutions of different duration and thus already included in the continuous evolutions of  $\forall i : A f(\mathbf{s})' = \theta$ . The (optional) iteration rule  $[*n]\square$  can partially unwind loops. It relies on rule  $[;]\square$ .

The dual rules  $\langle \cup \rangle \diamond, \langle ; \rangle \diamond, \langle := \rangle \diamond, \langle ? \rangle \diamond, \langle ' \rangle \diamond, \langle *^n \rangle \diamond$  work similarly. Rules for handling  $[\alpha] \diamond \phi$  and  $\langle \alpha \rangle \square \phi$  are discussed in Section 8.

The inductive definition rules  $[*] \square$  and  $\langle * \rangle \diamond$  completely reduce temporal properties of loops to QdTL properties of standard non-temporal QdL modalities such that standard induction (*ind*) or convergence (*con*) rules, as listed in Fig. 2, can be used for the outer non-temporal modality of the loop. Hence, after applying the inductive loop definition rules  $[*] \square$  and  $\langle * \rangle \diamond$ , the standard QdL loop invariant and variant rules can be used for verifying temporal properties of loops without change, except that the postcondition contains temporal modalities.

## 6.2 Soundness and Completeness

The following result shows that verification with the QdTL calculus always produces correct results about the safety of distributed hybrid systems, i.e., the QdTL calculus is sound.

**Theorem 1 (Soundness of QdTL).** *The QdTL calculus is sound, i.e., every QdTL (state) formula that can be proven is valid.*

The verification for temporal safety ( $[\alpha] \square \phi$  or  $\langle \alpha \rangle \diamond \phi$ ), temporal liveness ( $[\alpha] \diamond \phi$  or  $\langle \alpha \rangle \square \phi$ ), and non-temporal ( $[\alpha] \phi$  or  $\langle \alpha \rangle \phi$ ) fragments of distributed hybrid systems has *three independent sources* of undecidability. Thus, no verification technique can be effective. Hence, QdTL cannot be effectively axiomatizable. Both its discrete and its continuous fragments alone are subject to Gödel's incompleteness theorem [19]. The fragment with only structural and dimension-changing dynamics is not effective either, because it can encode two-counter machines.

QdL has been proved to be complete relative to quantified differential equations [21,22]. Due to the modular construction of the QdTL calculus, we can lift the relative completeness result from QdL to QdTL. We essentially show that QdTL is complete relative to QdL, which directly implies that QdTL calculus is even complete relative to an oracle for the fragment of QdTL that has only quantified differential equations in modalities. Again, we restrict our attention to homogeneous combinations of path and trace quantifiers like  $[\alpha] \square \phi$  or  $\langle \alpha \rangle \diamond \phi$ .

**Theorem 2 (Relative Completeness of QdTL).** *The calculus in Fig. 2 is a complete axiomatization of QdTL relative to quantified differential equations.*

This result shows that both temporal and non-temporal properties of distributed hybrid systems can be proven to exactly the same extent to which properties of quantified differential equations can be proven. It also gives a formal justification that the QdTL calculus reduces temporal properties to non-temporal QdL properties.

## 7 Verification of Distributed Air Traffic Control Safety Properties

Continuing the distributed air traffic control study from Section 5, the QdTL proofs of the temporal safety invariant in (1) and the temporal safety property in (2) are

presented in Fig. 3 and Fig. 4, respectively (for the purpose of simplifying the presentation, we ignore typing information  $A$  for aircraft in the proof, because it is clear from the context). Note that temporal and non-temporal properties of the maneuver cannot be proven using any hybrid systems verification technique, because the dimension is parametric and unbounded and may even change dynamically during the remainder of the maneuver. The single proof in Fig. 3 or Fig. 4 corresponds to infinitely many proofs for systems with  $n$  aircraft for all  $n$ .

Our proofs show that the distributed roundabout maneuver always safely avoids collisions for arbitrarily many aircraft (even with dynamic appearance of new aircraft). The above maneuver still requires all aircraft in the horizon of relevance to participate in the collision avoidance maneuver. In fact, we can show that this is unnecessary for aircraft that are far enough away and that may be engaged in other roundabouts. Yet, this is beyond the scope of this paper.

$$\begin{array}{c}
\text{true} \\
\mathbb{R} \frac{}{\forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j (2(x_1(i) - x_1(j))(-\omega(x_2(i) - x_2(j))) + 2(x_2(i) - x_2(j))\omega(x_1(i) - x_1(j)) \geq 0)} \\
\mathbb{R} \frac{}{\forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j (0 = 0 \wedge 2(x_1(i) - x_1(j))(d_1(i) - d_1(j)) + 2(x_2(i) - x_2(j))(d_2(i) - d_2(j)) \geq 0)} \\
[::=] \frac{}{\forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{L}(i)] \forall i, j (i' = j' \wedge 2(x_1(i) - x_1(j))(x_1(i)' - x_1(j)') + 2(x_2(i) - x_2(j))(x_2(i)' - x_2(j)') \geq 0)} \\
\\
\text{true} \\
\mathbb{R} \frac{}{\forall i, j (-\omega d_2(i) - (-\omega d_2(j)) = -\omega(d_2(i) - d_2(j)) \wedge \omega d_1(i) - \omega d_1(j) = \omega(d_1(i) - d_1(j)))} \\
[::=] \frac{}{[\forall i \mathcal{L}(i)] \forall i, j (d_1(i)' - d_1(j)' = -\omega(x_2(i)' - x_2(j)') \wedge d_2(i)' - d_2(j)' = \omega(x_1(i)' - x_1(j)'))} \\
\\
\begin{array}{cc}
[::=] \frac{}{[\forall i \mathcal{L}(i)] (\forall i, j \mathcal{T}(i, j))'} & [::=] \frac{}{\forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{L}(i)] (\forall i, j \mathcal{P}(i, j))'} \\
DI \frac{}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{F}_\omega(i)] \forall i, j \mathcal{T}(i, j)} & DI \frac{}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{F}_\omega(i) \& \forall i, j \mathcal{T}(i, j)] \forall i, j \mathcal{P}(i, j)} \\
DC \frac{}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{F}_\omega(i)] \forall i, j \mathcal{P}(i, j)} & \\
\hline
['] \square \frac{}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{F}_\omega(i)] \square \forall i, j \mathcal{P}(i, j)}
\end{array}
\end{array}$$

Abbreviation:  $\mathcal{L}(i) \equiv x_1(i)' := d_1(i), x_2(i)' := d_2(i), d_1(i)' := -\omega d_2(i), d_2(i)' := \omega d_1(i)$

Fig. 3: Proof for temporal collision freedom of roundabout collision avoidance maneuver circle

## 8 Liveness by Quantifier Alternation

Liveness specifications of the form  $[\alpha] \diamond \phi$  or  $\langle \alpha \rangle \square \phi$  are sophisticated ( $\Sigma_1^1$ -hard because they can express infinite occurrence in Turing machines). Beckert and Schlager [2], for instance, note that they failed to find sound rules for a discrete case that corresponds to  $[\alpha; \beta] \diamond \phi$ .

For *finitary liveness semantics*, we can still find proof rules. In this section, we modify the meaning of  $[\alpha] \diamond \phi$  to refer to all *terminating* traces of  $\alpha$ . Then, the straightforward generalization  $[\cdot] \diamond$  in Fig. 5 is sound, even in the hybrid case. But  $[\cdot] \diamond$  still leads to an incomplete axiomatization as it does not cover the case where, in some traces,  $\phi$  becomes true at some point during  $\alpha$ , and in other traces,  $\phi$  only becomes true during  $\beta$ . To overcome this limitation, we use a program transformation approach. We instrument the quantified hybrid program to monitor the

$$\begin{array}{c}
\mathbb{R} \frac{\text{true}}{\chi \wedge \forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j (2(x_1(i) - x_1(j))(-\omega(x_2(i) - x_2(j))) + 2(x_2(i) - x_2(j))\omega(x_1(i) - x_1(j)) \geq 0)} \\
\mathbb{R} \frac{\chi \wedge \forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j (0 = 0 \wedge 2(x_1(i) - x_1(j))(d_1(i) - d_1(j)) + 2(x_2(i) - x_2(j))(d_2(i) - d_2(j)) \geq 0)}{\chi \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{K}(i)] \forall i, j (i' = j' \wedge 2(x_1(i) - x_1(j))(x_1(i)' - x_1(j)') + 2(x_2(i) - x_2(j))(x_2(i)' - x_2(j)') \geq 0)} \\
[::=] \frac{\dots}{\dots} \\
\mathbb{R} \frac{\text{true}}{\chi \rightarrow \forall i, j (-\omega d_2(i) - (-\omega d_2(j)) = -\omega(d_2(i) - d_2(j)) \wedge \omega d_1(i) - \omega d_1(j) = \omega(d_1(i) - d_1(j)))} \\
[::=] \frac{\chi \rightarrow [\forall i \mathcal{K}(i)] \forall i, j (d_1(i)' - d_1(j)' = -\omega(x_2(i)' - x_2(j)') \wedge d_2(i)' - d_2(j)' = \omega(x_1(i)' - x_1(j)'))}{\dots} \\
\begin{array}{cc}
[::=] \frac{\dots}{\chi \rightarrow [\forall i \mathcal{K}(i)] (\forall i, j \mathcal{T}(i, j))'} & [::=] \frac{\dots}{\chi \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{K}(i)] (\forall i, j \mathcal{P}(i, j))'} \\
DI \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{M}(i) \& \chi] \forall i, j \mathcal{T}(i, j)}{DI \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{M}(i) \& \chi] \forall i, j \mathcal{P}(i, j)}{\dots}} & DI \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{M}(i) \& \chi \wedge \forall i, j \mathcal{T}(i, j)] \forall i, j \mathcal{P}(i, j)}{DI \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{M}(i) \& \chi] \forall i, j \mathcal{P}(i, j)}{\dots}} \\
\end{array} \\
\begin{array}{cc}
[']\square, [::=] \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{M}(i) \& \chi] \forall i, j \mathcal{P}(i, j)}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] [\forall i \mathcal{M}(i) \& \chi] \square \forall i, j \mathcal{P}(i, j)} & [?]\square, [::=] \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i \mathcal{M}(i) \& \chi] \forall i, j \mathcal{P}(i, j)}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] [\forall i \mathcal{M}(i) \& \chi] [?\eta] \square \forall i, j \mathcal{P}(i, j)} \\
[;]\square \frac{\dots}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] [\forall i \mathcal{M}(i) \& \chi; ?\eta] \square \forall i, j \mathcal{P}(i, j)} & [;]\square \frac{\dots}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] [\forall i \mathcal{M}(i) \& \chi; ?\eta] \square \forall i, j \mathcal{P}(i, j)} \\
\end{array} \\
\begin{array}{cc}
ax \frac{\text{true}}{\forall i, j \mathcal{P}(i, j), \forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j \mathcal{P}(i, j)} & ax \frac{\text{true}}{\forall i, j \mathcal{P}(i, j), \forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j \mathcal{P}(i, j)} \\
\wedge l \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow \forall i, j \mathcal{P}(i, j)}{[::=], \wedge l \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] \forall i, j \mathcal{P}(i, j)}{\dots}} & [::=], \wedge l \frac{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] \forall i, j \mathcal{P}(i, j)}{\dots} \\
[::=]\square \frac{\dots}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] \square \forall i, j \mathcal{P}(i, j)} & [::=]\square \frac{\dots}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] \square \forall i, j \mathcal{P}(i, j)} \\
\end{array} \\
[::=]\square \frac{\dots}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] \square \forall i, j \mathcal{P}(i, j)} \quad [::=]\square \frac{\dots}{\forall i, j \mathcal{P}(i, j) \wedge \forall i, j \mathcal{T}(i, j) \rightarrow [\forall i t := 0] [\forall i \mathcal{M}(i) \& \chi; ?\eta] \square \forall i, j \mathcal{P}(i, j)}
\end{array}$$

Abbreviations:

$$\begin{aligned}
\mathcal{M}(i) &\equiv \mathcal{F}_{\omega(i)}(i), t' = 1 \\
\chi &\equiv \forall i t \leq T \\
\eta &\equiv \forall i t = T \\
\mathcal{K}(i) &\equiv x_1(i)' := d_1(i), x_2(i)' := d_2(i), d_1(i)' := -\omega d_2(i), d_2(i)' := \omega d_1(i), t' := 1
\end{aligned}$$

Fig. 4: Proof for temporal collision freedom of roundabout collision avoidance maneuver circle in bounded time

occurrence of  $\phi$  during all changes: In  $[\alpha]\diamond$ ,  $\tilde{\alpha}$  results from replacing all occurrences of  $\forall i : A f(\mathbf{s}) := \theta$  with  $\forall i : A f(\mathbf{s}) := \theta; ?(\phi \rightarrow t = 1)$  and  $\forall i : A f(\mathbf{s})' = \theta \& \chi$  with  $\forall i : A f(\mathbf{s})' = \theta \& \chi \wedge (\phi \rightarrow t = 1)$ . The latter is a continuous evolution restricted to the region that satisfies  $\chi$  and  $\phi \rightarrow t = 1$ . The effect is that  $t$  detects whether  $\phi$  has occurred during any change in  $\alpha$ . In particular,  $t$  is guaranteed to be 1 after all runs if  $\phi$  occurs at least once along all traces of  $\alpha$ .

## 9 Conclusions and Future Work

For reasoning about distributed hybrid systems, we have introduced a temporal dynamic logic, QdTL, with modal path quantifiers over traces and temporal quantifiers along the traces. It combines the capabilities of quantified differential dynamic logic to reason about possible distributed hybrid system behavior with the

$$([\cdot] \diamond) \frac{\rightarrow [\alpha] \diamond \phi, [\alpha][\beta] \diamond \phi}{\rightarrow [\alpha; \beta] \diamond \phi} \quad ([\alpha] \diamond) \frac{\phi \vee \forall t : \mathbb{R} [\dot{\alpha}] t = 1}{[\alpha] \diamond \phi}$$

Fig. 5: Transformation rules for alternating temporal path and trace quantifiers

power of temporal logic in reasoning about the behavior along traces. Furthermore, we have presented a proof calculus for verifying temporal safety specifications of quantified hybrid programs in QdTL.

Our sequent calculus for QdTL is a completely modular combination of temporal and non-temporal reasoning. Temporal formulas are handled using rules that augment intermediate state transitions with corresponding sub-specifications. Purely non-temporal rules handle the effects of discrete transitions, continuous evolutions, and structural/dimension changes. The modular nature of the QdTL calculus further enables us to lift the relative completeness result from QdL to QdTL. This theoretical result shows that the QdTL calculus is a sound and complete axiomatization of the temporal behavior of distributed hybrid systems relative to differential equations. As an example, we demonstrate that our logic is suitable for reasoning about temporal safety properties in a distributed air traffic control system.

We are currently extending our verification tool for distributed hybrid systems, which is an automated theorem prover called KeYmaeraD [25], to cover the full QdTL calculus. Future work includes extending QdTL with CTL\*-like [10] formulas of the form  $[\alpha](\psi \wedge \Box \phi)$  to avoid splitting of the proof into two very similar sub-proofs for temporal parts  $[\alpha]\Box \phi$  and non-temporal parts  $[\alpha]\psi$  arising in  $[\cdot]\Box$ . Our combination of temporal logic with dynamic logic is more suitable for this purpose than the approach in [2], since QdTL has uniform modalities and uniform semantics for temporal and non-temporal specifications. This extension will also simplify the treatment of alternating liveness quantifiers conceptually.

## References

1. R. Alur, C. Courcoubetis, and D. L. Dill. Model-checking for real-time systems. In *LICS*, pages 414–425. IEEE Computer Society, 1990.
2. B. Beckert and S. Schlager. A sequent calculus for first-order dynamic logic with trace modalities. In R. Goré, A. Leitsch, and T. Nipkow, editors, *IJCAR*, volume 4130 of *LNCS*, pages 626–641. Springer, 2001.
3. E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. MIT Press, Cambridge, MA, USA, 1999.
4. W. Damm, H. Hungar, and E. R. Olderog. On the verification of cooperating traffic agents. In F. S. de Boer, M. M. Bonsangue, S. Graf, and W. P. de Roever, editors, *FMCO*, volume 3188 of *LNCS*, pages 77–110. Springer, 2003.
5. J. M. Davoren, V. Coulthard, N. Markey, and T. Moor. Non-deterministic temporal logics for general flow systems. In R. Alur and G. J. Pappas, editors, *HSCC*, volume 2993 of *LNCS*, pages 280–295. Springer, 2004.
6. J. M. Davoren and A. Nerode. Logics for hybrid systems. *Proceedings of the IEEE*, 88(7):985–1010, July 2000.
7. A. Deshpande, A. Göllü, and P. Varaiya. SHIFT: A formalism and a programming language for dynamic networks of hybrid automata. In *Hybrid Systems*, pages 113–133, 1996.



8. G. Dowek, C. Muñoz, and V. A. Carreño. Provably safe coordinated strategy for distributed conflict resolution. In *AIAA Proceedings, AIAA-2005-6047*, pages 278–292, 2005.
9. E. A. Emerson and E. M. Clarke. Using branching time temporal logic to synthesize synchronization skeletons. *Sci. Comput. Program*, 2(3):241–266, 1982.
10. E. A. Emerson and J. Y. Halpern. “Sometimes” and “Not Never” revisited: on branching versus linear time temporal logic. *J. ACM*, 33(1):151–178, 1986.
11. J. Faber and R. Meyer. Model checking data-dependent real-time properties of the European Train Control System. In *FMCAD*, pages 76–77. IEEE Computer Society Press, Nov 2006.
12. D. Harel, D. Kozen, and J. Tiuryn. *Dynamic logic*. MIT Press, Cambridge, 2000.
13. T. A. Henzinger. The theory of hybrid automata. In *LICS*, pages 278–292, 1996.
14. T. A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. In *LICS*, pages 394–406. IEEE Computer Society, 1992.
15. A. Hsu, F. Eskafi, S. Sachs, and P. Varaiya. Design of platoon maneuver protocols for IVHS. Technical Report PATH Research Report UCB-ITS-PRR-91-6, UC Berkeley, 1991.
16. F. Kratz, O. Sokolsky, G. J. Pappas, and I. Lee. R-Charon, a modeling language for reconfigurable hybrid systems. In *HSCC*, pages 392–406, 2006.
17. D. Leivant. Partial correctness assertions provable in dynamic logics. In I. Walukiewicz, editor, *FoSSaCS*, volume 2987 of *LNCS*, pages 304–317. Springer, 2004.
18. V. Mysore, C. Piazza, and B. Mishra. Algorithmic algebraic model checking II: Decidability of semi-algebraic model checking and its applications to systems biology. In D. Peled and Y. K. Tsay, editors, *ATVA*, volume 3707 of *LNCS*, pages 217–233. Springer, 2005.
19. A. Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reas.*, 41(2):143–189, 2008.
20. A. Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010.
21. A. Platzer. Quantified differential dynamic logic for distributed hybrid systems. In Anuj Dawar and Helmut Veith, editors, *CSL*, volume 6247 of *LNCS*, pages 469–483. Springer, 2010.
22. A. Platzer. Quantified differential dynamic logic for distributed hybrid systems. Technical Report CMU-CS-10-126, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, May 2010.
23. A. Pnueli. The temporal logic of programs. In *FOCS*, pages 46–57. IEEE, 1977.
24. V. R. Pratt. Process logic. In *POPL*, pages 93–100, 1979.
25. D. W. Renshaw, S. M. Loos, and A. Platzer. Distributed theorem proving for distributed hybrid systems. In Shengchao Qin and Zongyan Qiu, editors, *ICFEM*, volume 6991 of *LNCS*, pages 356–371. Springer, 2011.
26. C. Tomlin, G. J. Pappas, and S. Sastry. Conflict resolution for air traffic management: a study in multi-agent hybrid systems. *IEEE T. Automat. Contr.*, 43(4):509–521, 1998.
27. D. A. van Beek, K. L. Man, M. A. Reniers, J. E. Rooda, and R. R. H. Schiffelers. Syntax and consistent equation semantics of hybrid chi. *J. Log. Algebr. Program*, 68(1-2):129–210, 2006.

## A Proof of Conservative Temporal Extension

### A.1 Reachability Semantics of QdL

In this subsection, we review the reachability semantics of QdL given in [21,22] before proving Proposition 1 in the next subsection.

**Definition 4 (Reachability Semantics of QHP).** *The reachability semantics,  $\rho(\alpha)$ , of QHP  $\alpha$ , is a transition relation on states. It specifies which state  $\tau \in \mathcal{S}$  is reachable from a state  $\sigma \in \mathcal{S}$  by running QHP  $\alpha$  and is defined as:*

1.  $(\sigma, \tau) \in \rho(\forall i : A \ f(\mathbf{s}) := \theta)$  iff  $\tau$  is identical to  $\sigma$  except that at each position  $\mathbf{o}$  of  $f$ : if  $\sigma_i^e[\mathbf{s}] = \mathbf{o}$  for some object  $e \in \sigma(A)$ , then  $\tau(f)(\sigma_i^e[\mathbf{s}]) = \sigma_i^e[\theta]$ . If there are multiple objects  $e$  giving the same position  $\sigma_i^e[\mathbf{s}] = \mathbf{o}$ , then all of the resulting states  $\tau$  are reachable.
2.  $(\sigma, \tau) \in \rho(\forall i : A \ f(\mathbf{s})' = \theta \ \& \ \chi)$  iff there is a function  $\varphi : [0, r] \rightarrow \mathcal{S}$  for some  $r \geq 0$  with  $\varphi(0) = \sigma$  and  $\varphi(r) = \tau$  satisfying the following conditions. At each time  $t \in [0, r]$ , state  $\varphi(t)$  is identical to  $\sigma$ , except that at each position  $\mathbf{o}$  of  $f$ : if  $\sigma_i^e[\mathbf{s}] = \mathbf{o}$  for some object  $e \in \sigma(A)$ , then, at each time  $\zeta \in [0, r]$ :
  - The differential equations hold and derivatives exist (trivial for  $r = 0$ ):

$$\frac{d(\varphi(t)_i^e[f(\mathbf{s})])}{dt}(\zeta) = (\varphi(\zeta)_i^e[\theta])$$

– The evolution domains is respected:  $\varphi(\zeta)_i^e[\chi] = \text{true}$ .

If there are multiple objects  $e$  giving the same position  $\sigma_i^e[\mathbf{s}] = \mathbf{o}$ , then all of the resulting states  $\tau$  are reachable.

3.  $\rho(? \chi) = \{(\sigma, \sigma) : \sigma[\chi] = \text{true}\}$
4.  $\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$
5.  $\rho(\alpha; \beta) = \{(\sigma, \tau) : (\sigma, z) \in \rho(\alpha) \text{ and } (z, \tau) \in \rho(\beta) \text{ for a state } z.\}$
6.  $(\sigma, \tau) \in \rho(\alpha^*)$  iff there is an  $n \in \mathbb{N}$  with  $n \geq 0$  and there are states  $\sigma = \sigma_0, \dots, \sigma_n = \tau$  such that  $(\sigma_i, \sigma_{i+1}) \in \rho(\alpha)$  for all  $0 \leq i < n$ .

**Definition 5 (Valuation of QdL Formulas).** *The valuation of QdL formula  $\phi$  with respect to state  $\sigma$  is defined as follows:*

1.  $\sigma[\theta_1 = \theta_2] = \text{true}$  iff  $\sigma[\theta_1] = \sigma[\theta_2]$ ; accordingly for  $\geq$ .
2.  $\sigma[\phi \wedge \psi] = \text{true}$  iff  $\sigma[\phi] = \text{true}$  and  $\sigma[\psi] = \text{true}$ ; accordingly for  $\neg$ .
3.  $\sigma[\forall i : A \ \phi] = \text{true}$  iff  $\sigma_i^e[\phi] = \text{true}$  for all objects  $e \in \sigma(A)$ .
4.  $\sigma[\exists i : A \ \phi] = \text{true}$  iff  $\sigma_i^e[\phi] = \text{true}$  for some object  $e \in \sigma(A)$ .
5.  $\sigma[[\alpha]\phi] = \text{true}$  iff  $\tau[\phi] = \text{true}$  for all states  $\tau$  with  $(\sigma, \tau) \in \rho(\alpha)$ .
6.  $\sigma[\langle \alpha \rangle \phi] = \text{true}$  iff  $\tau[\phi] = \text{true}$  for some  $\tau$  with  $(\sigma, \tau) \in \rho(\alpha)$ .

### A.2 Extension Proof

The proof of Proposition 1 uses the following lemma about the relationship of reachability and trace semantics of QdTL programs, which agree on initial and final states.

**Lemma 1.** *For QHP  $\alpha$ , we have*

$$\rho(\alpha) = \{(\text{first } \nu, \text{last } \nu) : \nu \in \mu(\alpha) \text{ terminates.}\}$$

*Proof.* The proof follows an induction on the structure of  $\alpha$ .

- The cases  $\forall i : A \ f(\mathbf{s}) := \theta$ ,  $\forall i : A \ f(\mathbf{s})' = \theta \ \& \ \chi$ , and  $\alpha \cup \beta$  are simple by comparing the Definition 2 and Definition 4.
- For  $? \chi$ , the reasoning splits into two directions. For the direction “ $\supseteq$ ”, assume  $\nu \in \mu(? \chi)$ . We distinguish between two cases. If  $\text{first } \nu \llbracket \chi \rrbracket = \text{true}$ , then  $\nu = (\hat{\sigma})$  has length one,  $\text{last } \nu = \text{first } \nu$ , and  $(\text{first } \nu, \text{last } \nu) \in \rho(\alpha)$ . If, however,  $\text{first } \nu \llbracket \chi \rrbracket = \text{false}$ , then  $\nu = (\hat{\sigma}, \hat{A})$  does not terminate, hence, there is nothing to show. Conversely, for “ $\subseteq$ ”, assume  $(\sigma, \sigma) \in \rho(? \chi)$ , then  $\sigma \llbracket \chi \rrbracket = \text{true}$  and  $(\hat{\sigma}) \in \mu(? \chi)$  satisfies the conditions on  $\nu$ .
- For  $\alpha; \beta$  and the direction “ $\supseteq$ ”, assume that  $\nu \circ \varsigma \in \mu(\alpha; \beta)$  terminates with  $\nu \in \mu(\alpha)$ ,  $\varsigma \in \mu(\beta)$ , and  $\text{last } \nu = \text{first } \varsigma$ . Then, by induction hypothesis, we can assume that  $(\text{first } \nu, \text{last } \nu) \in \rho(\alpha)$ , and  $(\text{first } \varsigma, \text{last } \varsigma) \in \rho(\beta)$ . By the semantics of sequential composition, we conclude  $(\text{first } \nu \circ \varsigma, \text{last } \nu \circ \varsigma) \in \rho(\alpha; \beta)$ . Conversely, for “ $\subseteq$ ”, assume that  $(\sigma, \tau) \in \rho(\alpha; \beta)$ , i.e., let  $(\sigma, z) \in \rho(\alpha)$  and  $(z, \tau) \in \rho(\beta)$ . By induction hypothesis, there is a terminating trace  $\nu \in \mu(\alpha)$  with  $\text{first } \nu = \sigma$  and  $\text{last } \nu = z$ . Further, by induction hypothesis, there is a terminating trace  $\varsigma \in \mu(\beta)$  with  $\text{first } \varsigma = z$  and  $\text{last } \varsigma = \tau$ . Hence,  $\nu \circ \varsigma \in \mu(\alpha; \beta)$  terminates,  $\text{first } \nu \circ \varsigma = \sigma$  and  $\text{last } \nu \circ \varsigma = \tau$ .
- The case  $\alpha^*$  is an inductive consequence of the sequential composition case.

*Proof (of Proposition 1).* The formulas of  $\text{QdL}$  are a subset of the  $\text{QdTL}$  formulas. In the course of this proof, we use the notation  $\sigma_{\text{QdL}} \llbracket \cdot \rrbracket$  to indicate that the  $\text{QdL}$  valuation from Definition 5 is used. For  $\text{QdL}$  formulas  $\psi$ , we show that the valuations with respect to Definition 3 and with respect to Definition 5 are the same for all states  $\sigma$ :

$$\sigma \llbracket \psi \rrbracket = \sigma_{\text{QdL}} \llbracket \psi \rrbracket \text{ for all } \sigma.$$

We prove this by induction on the structure of  $\psi$ . The cases  $\theta_1 = \theta_2$ ,  $\theta_1 \geq \theta_2$ ,  $\neg \phi$ ,  $\phi \wedge \psi$ ,  $\forall i : A \ \phi$ ,  $\exists i : A \ \phi$  of state formulas are obvious. The other cases are proven as follows.

- If  $\psi$  has the form  $[\alpha] \phi$ , assume that  $\sigma \llbracket [\alpha] \phi \rrbracket = \text{false}$ . Then there is some terminating trace  $\nu \in \mu(\alpha)$  with  $\text{first } \nu = \sigma$  such that  $\text{last } \nu \llbracket \phi \rrbracket = \text{false}$ . By induction hypothesis, this implies that  $\text{last } \nu_{\text{QdL}} \llbracket \phi \rrbracket = \text{false}$ . According to Lemma 1,  $(\sigma, \text{last } \nu) \in \rho(\alpha)$  holds, which implies  $\sigma_{\text{QdL}} \llbracket [\alpha] \phi \rrbracket = \text{false}$ . For the converse direction, assume that  $\sigma_{\text{QdL}} \llbracket [\alpha] \phi \rrbracket = \text{false}$ . Then there is a  $(\sigma, \tau) \in \rho(\alpha)$  with  $\tau_{\text{QdL}} \llbracket \phi \rrbracket = \text{false}$ . By Lemma 1, there is a terminating trace  $\nu \in \mu(\alpha)$  with  $\text{first } \nu = \sigma$  and  $\text{last } \nu = \tau$ . By induction hypothesis,  $\text{last } \nu \llbracket \phi \rrbracket = \text{false}$ . Thus, we can conclude that both  $\nu \llbracket \phi \rrbracket = \text{false}$  and  $\nu \llbracket [\alpha] \phi \rrbracket = \text{false}$ .
- The case  $\psi = \langle \alpha \rangle \phi$  is proven accordingly.

## B Proof of Soundness and Completeness

### B.1 Proof of Soundness

*Proof (Proof of Theorem 1).* We show that all rules of the QdTL calculus are *locally sound*, i.e., for all states  $\sigma$ , the conclusion of a rule is true in state  $\sigma$  when all premisses are true in  $\sigma$ . Let  $\sigma$  be any state. For each rule we have to show that the conclusion is true in  $\sigma$  assuming the premisses are true in  $\sigma$ . Inductively, the soundness of the non-temporal rules follows from Proposition 1 and local soundness of the corresponding rules in QdL [21,22]. The proof for the generalization in  $\langle \cup \rangle$  and  $\langle \cup \rangle$  to path formulas  $\pi$  is a straightforward extension.

- $[\cdot] \Box$  Assume  $\sigma \models [\alpha] \Box \phi$  and  $\sigma \models [\alpha][\beta] \Box \phi$ . Let  $\nu \in \mu(\alpha; \beta)$ , i.e.,  $\nu = \varrho \circ \varsigma$  with first  $\nu = \sigma$ ,  $\varrho \in \mu(\alpha)$ , and  $\varsigma \in \mu(\beta)$ . If  $\varrho$  does not terminate, then  $\nu = \varrho \in \mu(\alpha)$  and  $\nu \models \Box \phi$  by premise. If  $\varrho$  terminates with last  $\varrho = \text{first } \varsigma$ , then  $\varrho \models \Box \phi$  by premise. Further, we know  $\sigma \models [\alpha][\beta] \Box \phi$ . In particular for trace  $\varrho \in \mu(\alpha)$ , we have last  $\varrho \models [\beta] \Box \phi$ . Thus,  $\varsigma \models \Box \phi$  because  $\varsigma \in \mu(\beta)$  starts at first  $\varsigma = \text{last } \varrho$ . By composition,  $\varrho \circ \varsigma \models \Box \phi$ . As  $\nu = \varrho \circ \varsigma$  was arbitrary, we can conclude  $\sigma \models [\alpha; \beta] \Box \phi$ . The converse direction holds, as all traces of  $\alpha$  are prefixes of traces of  $\alpha; \beta$ . Hence, the assumption  $\sigma \models [\alpha; \beta] \Box \phi$  directly implies  $\sigma \models [\alpha] \Box \phi$ . Further, all traces of  $\beta$  that begin at a state reachable from  $\sigma$  by  $\alpha$  are suffixes of traces of  $\alpha; \beta$  that start in  $\sigma$ . Hence,  $\sigma \models [\alpha][\beta] \Box \phi$  is implied as well.
- $[?] \Box$  Soundness of  $[?] \Box$  is obvious, since, by premise, we can assume  $\sigma \models \phi$ , and there is nothing to show for  $\Lambda$  states according to Definition 3. Conversely,  $\hat{\sigma}$  is a prefix of all traces in  $\mu(? \chi)$  that start in  $\sigma$ .
- $[\cdot] = \Box$  Assuming  $\sigma \models \phi$  and  $\sigma \models [\forall i : A f(\mathbf{s}) := \theta] \phi$ , we have to show that  $\sigma \models [\forall i : A f(\mathbf{s}) := \theta] \Box \phi$ . Let  $\nu \in \mu(\forall i : A f(\mathbf{s}) := \theta)$  be any trace with first  $\nu = \sigma$ , i.e.,  $\nu = (\hat{\sigma}, \hat{\tau})$  by Definition 2. Hence, the only two states we need to consider are  $\nu_0(0) = \sigma$  and  $\nu_1(0) = \tau$ . By premise,  $\nu_0(0) = \sigma$  yields  $\nu_0(0) \models \phi$ . Similarly, for the state  $\nu_1(0) = \text{last } \nu = \tau$ , the premise gives  $\nu_1(0) \models \phi$ . The converse direction is similar.
- $['] \Box$  We prove that  $['] \Box$  is locally sound by contraposition. For this, assume that  $\sigma \not\models [\forall i : A f(\mathbf{s})' = \theta \ \& \ \chi] \Box \phi$ ; then there is a trace  $\nu = (\varphi) \in \mu(\forall i : A f(\mathbf{s})' = \theta \ \& \ \chi)$  starting in first  $\nu = \sigma$  and  $\sigma \not\models \Box \phi$ . Hence, there is a position  $(0, \zeta)$  of  $\nu$  with  $\nu_0(\zeta) \not\models \phi$ . Now  $\varphi$  restricted to  $[0, \zeta]$  also solves the quantified differential equation  $\forall i : A f(\mathbf{s})' = \theta \ \& \ \chi$ . Thus,  $(\varphi|_{[0, \zeta]}) \not\models \phi$  as  $\varphi(\zeta) \not\models \phi$ , since the last state is  $\varphi(\zeta)$ . By consequence, this gives  $\sigma \not\models [\forall i : A f(\mathbf{s})' = \theta \ \& \ \chi] \phi$ . The converse direction is obvious as last  $\nu$  always is a state occurring during  $\nu$ . Hence,  $\sigma \not\models [\forall i : A f(\mathbf{s})' = \theta \ \& \ \chi] \phi$  immediately implies  $\sigma \not\models [\forall i : A f(\mathbf{s})' = \theta \ \& \ \chi] \Box \phi$ .
- $[*^n] \Box$  By contraposition, assume that  $\sigma \not\models [\alpha^*] \Box \phi$ . Then there is an  $n \in \mathbb{N}$  and a trace  $\nu \in \mu(\alpha^n)$  with first  $\nu = \sigma$  such that  $\nu \not\models \Box \phi$ . There are two cases. If  $n > 0$  then  $\nu \in \mu(\alpha; \alpha^*)$ , and thus  $\sigma \not\models [\alpha; \alpha^*] \Box \phi$ . If, however,  $n = 0$ , then  $\nu = (\hat{\sigma})$  and  $\sigma \not\models \phi$ . Hence, all traces  $\varsigma \in \mu(\alpha; \alpha^*)$  with first  $\varsigma = \sigma$  satisfy  $\varsigma \not\models \Box \phi$ . Finally, it is easy to see that all programs have at least one such trace  $\varsigma$  that witnesses  $\sigma \not\models [\alpha; \alpha^*] \Box \phi$ . The converse direction is easy as all behaviour of  $\alpha; \alpha^*$  is subsumed by  $\alpha^*$ , i.e.,  $\mu(\alpha; \alpha^*) \subseteq \mu(\alpha^*)$ .

- $[*]\Box$  Clearly, using the fact that  $\mu(\alpha^*) \supseteq \mu(\alpha^*; \alpha)$ , the set of states along the traces of  $\alpha^*$  at which  $\phi$  needs to be true for the premise is a subset of the corresponding set for the conclusion. Hence, the conclusion entails the premise. Conversely, all states during traces of  $\alpha^*$  are also reachable by iterating  $\alpha$  sufficiently often to completion and then following a single trace of  $\alpha$ . In detail: If  $\sigma \not\models [\alpha^*]\Box\phi$ , then there is a trace  $\nu \in \mu(\alpha^*)$  on which  $\neg\phi$  holds true at some state, say, at  $\nu_k(\zeta) \neq \perp$ . Let  $n \geq 0$  be the (maximum) number of complete repetitions of  $\alpha$  along  $\nu$  before discrete step index  $k$ . That is, there is some discrete step index  $k_n < k$  such that the prefix  $\varrho = (\nu_0, \dots, \nu_{k_n}) \in \mu(\alpha^n)$  of  $\nu$  consists of  $n$  complete repetitions of  $\alpha$  and the suffix  $\varsigma = (\nu_{k_n+1}, \nu_{k_n+2}, \dots) \in \mu(\alpha^*)$  starts with a trace of  $\alpha$  during which  $\neg\phi$  occurs at point  $\nu_k(\zeta)$ , namely at relative position  $(k - (k_n + 1), \zeta)$ . Let  $\zeta \in \nu(\alpha)$  be this prefix of  $\varsigma$ . Consequently,  $\zeta \models \langle \alpha \rangle \Diamond \neg\phi$  and the trace  $\varrho \circ \zeta$  is a witness for  $\sigma \models \langle \alpha^* \rangle \langle \alpha \rangle \Diamond \neg\phi$ .

The proofs for  $\langle ; \rangle \Diamond \langle * \rangle \Diamond$  are dual, since  $\langle \alpha \rangle \Diamond \phi$  is equivalent to  $\neg[\alpha]\Box\neg\phi$  by duality.

## B.2 Proof of Relative Completeness

*Proof (Outline of Proof of Theorem 2).* The proof is a simple extension of the proof of Theorem 1 in [22], which is the relative completeness theorem for QdL, because the QdTL calculus successively reduces temporal properties to non-temporal properties and, in particular, handles loops by inductive definition rules in terms of QdL modalities. The temporal rules in Fig. 2 transform temporal formulas to simpler formulas, i.e., to where the temporal modalities occur after simpler programs ( $[\cup]\Box$ ,  $[*]\Box$ ,  $\langle \cup \rangle \Diamond$ ,  $\langle * \rangle \Diamond$ ) or disappear completely ( $[?]\Box$ ,  $[:=]\Box$ ,  $[']\Box$  and  $\langle ? \rangle \Diamond$ ,  $\langle := \rangle \Diamond$ ,  $\langle ' \rangle \Diamond$ ). Hence, the inductive relative completeness proof for QdL in [22] directly generalizes to QdTL with the following addition: After applying  $[*]\Box$  or  $\langle * \rangle \Diamond$ , loops are ultimately handled by the standard QdL rules *ind* and *con*. To show that sufficiently strong invariants and variants exist for the temporal postconditions  $[\alpha]\Box\phi$  and  $\langle \alpha \rangle \Diamond \phi$ , we only have to show that such temporal formulas are expressible in the *first-order logic of quantified differential equations*, FOQD [22].

## C Proofs for Liveness Verification by Quantifier Alternation

In this section, we prove that the rules in Section 8 are sound.

**Proposition 2 (Local soundness).** *The rules in Section 8 are locally sound for finitary liveness semantics.*

*Proof.* Let  $\sigma$  be any state.

- $[\cdot] \diamond$  Assuming that the premiss is true, we need to consider two cases corresponding to the two formulas of its succedent. If  $\sigma \models [\alpha] \diamond \phi$ , then obviously  $\sigma \models [\alpha; \beta] \diamond \phi$ , as every trace of  $\alpha; \beta$  has a trace of  $\alpha$  as prefix, during which  $\phi$  holds at least once. If, however,  $\sigma \models [\alpha][\beta] \diamond \phi$ , then  $\phi$  occurs at least once during all traces that start in a state reachable from  $\sigma$  by  $\alpha$ . Let  $\varrho \circ \varsigma \in \mu(\alpha; \beta)$  with first  $\varrho = \sigma$ ,  $\varrho \in \mu(\alpha)$  and  $\varsigma \in \mu(\beta)$ . In finitary liveness semantics,  $\varrho \circ \varsigma$  can be assumed to terminate (otherwise there is nothing to show). Then, last  $\varrho$  is a state reachable from  $\sigma$  by  $\alpha$ , hence  $\varsigma \models \diamond \phi$ . Thus,  $\varrho \circ \varsigma \models \diamond \phi$ .
- $[\alpha] \diamond$  For the soundness of  $[\alpha] \diamond$ , first observe that the truth of  $\sigma \llbracket \phi \rrbracket$  of  $\phi$  depends on the state  $\sigma$ , hence it can only be affected during state changes. Further, the only actual changes of valuations happen during discrete jumps  $\forall i : A f(\mathbf{s}) := \theta$  or continuous evolutions  $\forall i : A f(\mathbf{s})' = \theta \& \chi$ . All other system actions only cause control flow effects but no elementary state changes. Assume the premiss is true in a state  $\sigma$ . If  $\sigma \models \phi$ , the conjecture is obvious. Hence, assume  $\sigma \models \forall t : \mathbb{R} [\tilde{\alpha}] t = 1$ . Suppose  $\sigma \not\models [\alpha] \phi$ ; then there is a trace  $\nu \in \mu(\alpha)$  with  $\nu \not\models \diamond \phi$ . Then, this trace directly corresponds to a trace  $\tilde{\nu}$  of  $\tilde{\alpha}$  in which all  $\phi \rightarrow t = 1$  conditions are trivially satisfied as  $\phi$  never holds. As there are no changes of the fresh variable  $t$  during  $\tilde{\alpha}$ , the value of  $t$  remains constant during  $\tilde{\nu}$ . But then we can conclude that there is a trace, which is essentially the same as  $\tilde{\nu}$  except for the constant valuation of the fresh variable  $t$  on which no conditions are imposed, hence  $t = 0$  is possible. As these traces terminate in finitary liveness semantics, we can conclude  $\sigma \not\models \forall t : \mathbb{R} [\tilde{\alpha}] t = 1$ , which is a contradiction. Conversely for equivalence of premiss and conclusion, assume  $\sigma \not\models \phi \vee \forall t : \mathbb{R} [\tilde{\alpha}] t = 1$ . Then, the initial state  $\sigma$  does not satisfy  $\phi$  and it is possible for  $\tilde{\alpha}$  to execute along a terminating trace  $\nu$  that permits  $t$  to be  $\neq 1$ . Suppose there was a position  $(k, \zeta)$  of  $\nu$  at which  $\nu_k(\zeta) \models \phi$ . Without loss of generality, we can assume  $(k, \zeta)$  to be the first such position. Then, the hybrid action which regulates  $\nu_k$  is accompanied by an immediate condition that  $\varphi \rightarrow t = 1$ , hence  $t = 1$  holds if  $\nu$  terminates. Since the fresh variable  $t$  is rigid (is never changed during  $\tilde{\alpha}$ ) and  $\nu$  terminates in finitary liveness semantics, we conclude last  $\nu \llbracket t \rrbracket = 1$ , which is a contradiction.